

IN THE CLAIMS:

1. (currently amended) A method for securing network-connected resources, the method comprising:

at a first network-connected node, receiving an unencrypted electronically formatted job;

receiving CK, a symmetrical encryption key (K) encrypted using an asymmetrical encryption public key (pubK);

receiving CH, a hash (H) of the job, further encrypted using K;

decrypting CK using an asymmetrical encryption private key (privK), corresponding to pubK, to recover K;

hashing the job, generating H';

using K to validate CH;

in response to validating CH, decrypting an encrypted resource using K; and,

using the decrypted resource to process the job.

2. (original) The method of claim 1 wherein using K to validate CH includes:

encrypting H' using K, obtaining CH'; and,
matching CH to CH'.

3. (original) The method of claim 1 wherein using K to validate CH includes:

decrypting CH using K, generating H; and,
comparing H to H'.

4. (original) The method of claim 1 further comprising:

prior to receiving the job, CK, and CH, receiving the encrypted resource; and,

storing the encrypted resource.

5. (original) The method of claim 4 further comprising:

installing pubK,privK upon initialization.

6. (currently amended) The method of claim 1 wherein receiving [[an]] the unencrypted electronically formatted job includes receiving a print job in a format selected from the group including text and image formats.

7. (original) The method of claim 4 wherein storing the encrypted resource includes storing an encrypted font resource; and, wherein using the decrypted resource to process the job includes printing a print job using the decrypted fonts.

8. (original) The method of claim 7 wherein storing the encrypted font resource includes storing resources selected from the group including a logo, personal signature image, and glyph.

9. (original) The method of claim 4 wherein receiving the encrypted resource includes receiving the encrypted resource in a

format selected from the group including hypertext transport protocol (http) and file transport protocol (FTP).

10. (original) The method of claim 1 further comprising:

at a second network-connected node, generating the job;
encrypting K with pubK, generating CK;
hashing the job, generating H;
encrypting H using K, generating CH; and,
sending the job, CK, and CH to the first node for job

processing.

11. (original) The method of claim 1 further comprising:

receiving a selection command for a particular one of a plurality of encrypted resources; and,
wherein decrypting an encrypted resource using K, in response to a valid match, includes decrypting the selected resource.

12. (original) The method of claim 11 wherein receiving a selection command for a particular one of a plurality of encrypted resources includes receiving CK_i, where 1 ≤ i ≤ m; and,

wherein decrypting the selected resource in response to the encrypted resource selection command includes decrypting CK_i to recover one of symmetrical encryption keys K₁ through K_m, where K₁ through K_m correspond to encrypted resources CR₁ through CR_m.

13. (currently amended) The method of claim 1
wherein receiving [[an]] the unencrypted electronically formatted job
includes receiving the job at network-connected node N_i , where $1 \leq i \leq n$;
wherein receiving CK includes N_i receiving CK_i , where CK_i is
generated by encrypting K using corresponding asymmetrical encryption
public key $pubK_i$; and,
wherein decrypting CK includes N_i decrypting CK_i using
corresponding asymmetrical encryption private key $privK_i$, to recover K.

14. (currently amended) The method of claim 1
wherein receiving [[an]] the unencrypted electronically formatted job
includes receiving the job at network-connected node N_i , where $1 \leq i \leq n$;
wherein receiving CK includes N_i receiving CK_i ,
corresponding to symmetrical encryption key K_i , encrypted using $pubK_i$;
wherein receiving CH includes N_i receiving CH_i , a hash of
the job encrypted using corresponding symmetrical encryption key K_i ;
and;
wherein decrypting CK includes N_i decrypting CK_i using
asymmetrical encryption private key $privK_i$, to recover corresponding
symmetrical encryption key K_i .

15. (original) The method of claim 14 wherein using K
to validate CH includes:
 N_i encrypting H' using symmetrical encryption key K_i ,
obtaining CH'_i ;
 N_i matching CH_i to corresponding CH'_i ; and,

wherein decrypting an encrypted resource using K includes
Ni decrypting the encrypted resource using symmetrical encryption key
Ki.

16. (original) The method of claim 14 wherein using K
to validate CH includes:

Ni decrypting CHi using symmetrical encryption key Ki,
obtaining H;

Ni comparing H to H'; and,

wherein decrypting an encrypted resource using K includes
Ni decrypting the encrypted resource using symmetrical encryption key
Ki.

17. (currently amended) A method for accessing
network-connected processing resources, the method comprising:

at a second node, generating an unencrypted electronically
formatted job;

encrypting a symmetrical encryption key K with an
asymmetrical encryption key (pubK), generating CK;

hashing the job generating H;

encrypting H using K, generating CH;

sending the job, CK, and CH to a first network-connected
node; and,

processing the job at the first node using a K encrypted
resource.

18. (currently amended) A system for using secure network-connected resources, the system comprising:

- a first device including:
 - a network-connected port for receiving an unencrypted electronically formatted job, for receiving CK, a symmetrical encryption key (K) encrypted using an asymmetrical encryption public key (pubK), and for receiving CH, a hash (H) of the job, further encrypted using K;
 - a hash unit having an interface to accept the job and to supply a hash of the job (H');
 - a memory having an interface to supply an asymmetrical encryption private key (privK), corresponding to pubK, and an encrypted resource;
 - a security unit having an interface to authorize access to the encrypted resource in memory, in response to validating CH; and,
 - a processing unit having an interface to accept the job and a decrypted resource, and to supply a job processed using the decrypted resource.

19. (original) The system of claim 18 further comprising:

- a decrypting unit having an interface to accept CK and privK, to generate K in response to decrypting CK using privK, to decrypt the encrypted resource from memory using K, and supply the decrypted resource;
- an encryption unit having an interface to accept H' and K, and supply CH' in response to using K to encrypt H'; and,

wherein the security unit accepts CH and CH' and validates CH by matching CH to CH'.

20. (original) The system of claim 18 further comprising:

a decrypting unit having an interface to accept CH, CK, and privK, to generate K in response to decrypting CK using privK, to supply H in response to decrypting CH using K, and supply the decrypted resource; and,

wherein the security unit accepts H and H' and validates CH by matching H to H'.

21. (original) The system of claim 18 wherein the network-connected port receives the encrypted resource for storage in the memory.

22. (original) The system of claim 18 wherein the memory is a read only memory (ROM) for accepting and storing privK upon device initialization.

23. (original) The system of claim 18 wherein the first device is a printer; and,

wherein the network-connected port receives a print job in a format selected from the group including text and image formats.

24. (original) The system of claim 23 wherein the memory stores encrypted font resources; and,

wherein the processing unit is a print engine that supplies a job printed using the decrypted fonts.

25. (original) The system of claim 24 wherein the memory stores encrypted font resources selected from the group including a logo, personal signature image, and glyph.

26. (original) The system of claim 21 wherein the network-connected port receives an encrypted resource for storage in a format selected from the group including hypertext transport protocol (http) and file transport protocol (FTP).

27. (original) The system of claim 18 further comprising:

a second device including:

a processor to supply a job;

a hash unit having an interface to accept the job

and to supply a hash of the job (H);

an encryption unit having an interface to accept

H, to supply CK, the encryption of symmetrical encryption key K

using pubK, and CH, the encryption of H using K; and,

a network-connected port for transmitting the job, CK, and

CH to the first device for job processing.

28. (original) The system of claim 18 wherein the first device network-connected port receives a encrypted resource selection command; and,

wherein the decryption unit decrypts the selected resource.

29. (original) The system of claim 28 wherein the decryption unit decrypts CK_i , where $1 \leq i \leq m$, to recover one of symmetrical encryption keys K_1 through K_m , where K_1 through K_m correspond to encrypted resources CR_1 through CR_m .

30. (currently amended) The system of claim 18 further comprising:

a plurality of devices N_i , where $1 \leq i \leq n$, each receiving the unencrypted electronically formatted job at a network-connected port, along with CK_i , where CK_i is generated by encrypting K using corresponding asymmetrical encryption public key $pubK_i$; and,

wherein each device decryption unit decrypts CK_i using corresponding asymmetrical encryption private key $privK_i$, to recover K .

31. (currently amended) The method of claim 18 further comprising:

a plurality of devices N_i , where $1 \leq i \leq n$, each receiving the unencrypted electronically formatted job at a network-connected port, along with CK_i , where CK_i is generated by encrypting K_i using corresponding asymmetrical encryption public key $pubK_i$, and CH_i , a hash of the job encrypted using corresponding symmetrical encryption key K_i ; and,

wherein each device includes a decryption unit for decrypting CK_i using asymmetrical encryption private key $privK_i$, to recover

corresponding symmetrical encryption key K_i , for the decryption of the encrypted resource.

32. (original) The system of claim 31 wherein each device encryption unit encrypts H' using symmetrical encryption key K_i , obtaining CH'_i ; and,

wherein each device security unit validates CH by matching CH_i to corresponding CH'_i .

33. (original) The system of claim 31 wherein each device decryption unit decrypts CH_i using symmetrical encryption key K_i , obtaining H ; and,

wherein each device security unit validates CH by matching H to H' .

34. (currently amended) A system for accessing network-connected processing resources, the system comprising:

a second device including:

a processor to supply an unencrypted job;

a hash unit having an interface to accept the job

and to supply a hash of the job (H);

an encryption unit having an interface to accept

H , to supply CK , the encryption of symmetrical encryption key K using $pubK$, and CH , the encryption of H using K ; and,

a network-connected port for transmitting the job, CK , and CH to a first device for job processing.